REMARKS

In an Office Action dated 01 July 2005, the Examiner objected to the specification, Abstract, Title, and rejected claims 4 and 5 under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. In addition, the Examiner rejected claim 4 under 35 U.S.C. §112, second paragraph because of insufficient antecedent basis for the limitation "The first owner key" in line 21. In addition, the Examiner rejected claims 1 – 5, 10 – 14, 16, and 17 as best understood under 35 U.S.C. §102(b) as being anticipated by Chang et al. (US Patent No. 5,724,425). In addition, the Examiner rejected claims 6 – 9, 16, and 18 under 35 U.S.C. §103(a) as being unpatentable over Chang et al. (US Patent No. 5,724,425) as applied to claim 1 above, and further in view of Horstmann (US Patent No. 6,044,469).

The Examiner objected to the specification, Abstract, Title, and rejected claims 4 and 5 under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. In addition, the Examiner rejected claim 4 under 35 U.S.C. §112(b) because of insufficient antecedent basis for the limitation "The first owner key" in line 21. Appropriate amendments have been made to the specification, Title, Abstract and claim 4 to overcome the Examiner's objections and rejection of claims 4 and 5 under 35 U.S.C. §112 second paragraph.

The Examiner rejected claims 1 – 5, 10 – 14, 16, and 17 as best understood under 35 U.S.C. §102(b) as being anticipated by Chang et al. (US Patent No. 5,724,425). In addition, the Examiner rejected claims 6 – 9, 16, and 18 under 35 U.S.C. §103(a) as being unpatentable over Chang et al. (US Patent No. 5,724,425) as applied to claim 1 above, and further in view of Horstmann (US Patent No. 6,044,469). The Examiner noted:

> Regarding claims 1, 2, and 3: Hashing a file to produce a hash value (Col 7 lines 1-20) a message digest is used to describe the process of hashing the file. Chang et al. states that any known message digest algorithm such as MD2, MD4, or MD5 may be used in the creation of the digest. These algorithms hash the file in this same manner as described by the applicant thus providing for a hash value as the resultant. Encrypting the hash value with a key to generate a signature (Col 7 lines 1-5). Comparing the generated signature with the original (Fig 6(a, b), Col 9 lines 37-47) Chang et al states that the file is hashed (i.e. message digest generated) and the signature is decrypted to provide the original hash value. In this manner Chang et al provides for that which is claimed since these are to same thing by way of a logical

transitive relationship. Encrypting the newly generated hash value and comparing that to the provided signature is logically the same as decrypting the original signature and comparing that to the produced hash value.

Applicant has carefully reviewed the Examiner's rejections and the cited Chang reference. Applicant has amended the independent claims to distinguish Applicant's invention from the teachings of the cited references and provides the following remarks in support of patentability of the claimed invention.

Applicant's secure data authentication apparatus provides a method for authenticating the source of a software file as well as the owner of the software file and the telephony switching system the software file is being installed on. The software file is hashed using a selected hash algorithm. The hash value is then encrypted with the unique owner key to calculate a source signature. The benefit of creating a unique owner signature to append to the installation software is to prevent unauthorized individuals that obtain the software file in an unscrambled form from using the software file without authorization. Once calculated, the source signature and/or unique owner signature are appended to the software file. A secure microprocessor is located within the telephony switching equipment and includes an encryption algorithm, a security routine, a source key, and the unique owner key that are used by the secure microprocessor to calculate a source signature and a unique owner signature for each software file or downloaded image. The secure microprocessor compares the calculated source and owner signatures to the source and owner signatures appended to the end of the software file or images. If the signatures match, installation and use is authorized. If the signatures do not match, the software file cannot be installed and the telephony switching system may be disabled.

The use of an owner's key that is unique to each telephony switching system, which unique owner's key is used to encrypt the hash value at the source and also at the secure processor at the

Serial No. 10/028,004
Amendments And Remarks Responsive To
    Office Action Mailed 07/01/2005
Page 16 of 17
222108v1

telephony switching system is neither shown or suggested by the cited references. This limitation is now clearly recited in the independent claims, claim 1 of which is an example:

1.   A secure data authentication apparatus to authenticate a software file, the software file having a first signature appended to the software file, for use on a computer system, wherein said computer system is assigned an owner key that is unique to said computer system, said first signature comprising a source hash value that is computed by processing at least some of said software file using a selected hash function, which source hash value is encrypted using said owner key to produce said first signature, the apparatus comprising:

a secure processing device within the computer system to receive the software file and hash the software file using said selected hash function to produce a first hash value; and

a first key located within the secure processing device, which first key comprises said owner key wherein the secure processing device encrypts the first hash value with the first key to generate a second signature and compares the first signature with the second signature, and if the first signature matches the second signature, the computer system accepts the software file as being authenticated.

Applicant therefore believes that claims 1-18 are allowable under §102(b) and §103(a) over the cited references for the reasons noted above.

In view of the above amendments and remarks, Applicant believes the pending application is in condition for allowance. Applicant believes no fee is due with this response. However, if a fee is due, please charge our Deposit Account No. 50-1602, under Order No. 013217.0177PTUS from which the undersigned is authorized to draw.

Respectfully submitted,
PATTON BOGGS LLP

Dated: _____10/3/05_____

By: _____
James M. Graziano
Registration No.: 28,300
(303) 830-1776
(303) 894-9239 (Fax)
Attorney for Applicant

Customer No. 24283

Serial No. 10/028,004
Amendments And Remarks Responsive To
    Office Action Mailed 07/01/2005
Page 17 of 17
218373v1